UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/522,067	10/04/2005	Christopher Ian Blake	BLAKE	7581

23643 7590 07/16/2007

BARNES & THORNBURG LLP
11 SOUTH MERIDIAN
INDIANAPOLIS, IN 46204

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
07/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/522,067	BLAKE, CHRISTOPHER IAN	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 January 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/4/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 10/4/2005 but is a 371 case of PCT/AU03/00934 application filed 7/23/2003 and has a foreign priority application filed on 7/24/2002.

Preliminary Amendment

2. Examiner acknowledges Preliminary Amendment for the claims filed 1/21/2005. Applicants have amended pending claims 7, 10, 20, 23 26 and 27 to put the claims in proper form for examination. The submitted amendments have been entered and made of record. Presently, pending claims are 1 – 31.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 5 – 8, 10, 11 and 14 are rejected under 35 U.S.C. 102(b) as being anticipated by Albert et al. (U.S. Patent 5,991,410).

As per claim 1, Albert teaches a method of providing secure transmissions from a smartcard reader (Albert: Column 5 Line 29 / Line 38 – 39 & Figure 2 / Element 102), said method comprising the steps of:

encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information (Albert: Column 5 Line 27 – 29, Column 17 Line 4 – 6 and Column 12 Line 40: (a) a signal, e.g. the identifying data associated with the smart card user, is encrypted wherein the signal is indeed created differently per each smartcard and (b) the signal can be encrypted and / or compressed);

transmitting said encrypted signal to a remote location relative to said smartcard reader (Albert: Column 17 Line 7 – 11 & Figure 2 / Element 500: an host computer at a remote location via a wireless network relative to said smartcard reader);

translating at said remote location said transmitted signal to another format useable by an access controller (Albert: Abstract Line 10 – 12 and Column 18 Line 55 – 57 / Line 62 – 63: an authorization processor is an access controller and the host computer transforms the format between the PSTN non-compatible format and PSTN compatible format (i.e. recovered digital data format)); and

controlling an access mechanism using said access controller dependent upon said translated signal (Albert: Column 18 Line 65 – 67: based on the translated signal received from said authorization processor at said host computer signals to determine the authorization or denial of a transaction – i.e. access control mechanism).

As per claim 5, Albert teaches providing access using said access mechanism if said translated signal is determined by said access controller to authorize access (Albert: Column 18

Line 62 – 67: the recovered digital data signal format is communicated with authorization processor to authorize access).

As per claim 6, Albert teaches said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation (Albert: Column 18 Line 62 – 67).

As per claim 7, Albert teaches said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code (Albert: Column 5 Line 24 – 29).

As per claim 8, Albert teaches said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption (Albert: Column 12 Line 40).

As per claim 10, Albert teaches said encrypted signal is transmitted from said smartcard reader to a high security module at said remote location (Albert: Column 18 Line 55 – 57: the host computer is the high security module).

As per claim 11, Albert teaches said high security module translates said encrypted signal to said other format (Albert: Column 18 Line 62 – 63 & Abstract Line 10 – 12: the host computer transform the format between the PSTN non-compatible format and PSTN compatible format (i.e. recovered digital data format)).

As per claim 14, Albert teaches said translated signal is in a controller-specified format (Albert: Column 18 Line 62 – 63 & Abstract Line 10 – 12: the host computer transform the

format between the PSTN non-compatible format and PSTN compatible format (i.e. recovered digital data format) and thus the translated signal is the recovered digital data format, which is a PSTN compatible format used by authorization processor, i.e. access controller).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 2 – 4, 9, 16 – 24, 27 and 29 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Baratelli (U.S. Patent 6,325,285).

As per claim 16 and 29, Albert teaches a system for providing secure transmissions from a smartcard reader (Albert: Column 5 Line 29 / Line 38 – 39 & Figure 2 / Element 102), said system comprising:

a high security module for receiving said transmitted signal and translating said transmitted signal to another format useable by an access controller (Albert: Abstract Line 10 – 12 and Column 18 Line 55 – 57 / Line 62 – 63: (a) the host computer is the high security module and an authorization processor is an access controller (b) the host computer transforms the format between the PSTN non-compatible format and PSTN compatible format (i.e. recovered digital data format)); and

an access controller for controlling an access mechanism using said access controller dependent upon said translated signal (Albert: Column 18 Line 65 – 67: based on the translated signal received from said authorization processor at said host computer signals to determine the authorization or denial of a transaction – i.e. access control mechanism);

encrypting a signal created by said smartcard reader dependent on said smartcard, said signal comprising access information (Albert: Column 5 Line 27 – 29, Column 17 Line 4 – 6 and Column 12 Line 40: (a) a signal, e.g. the identifying data associated with the smart card user, is encrypted wherein the signal is indeed created differently per each smartcard and (b) the signal can be encrypted and / or compressed), and for transmitting said encrypted signal to a remote location relative to said smartcard reader (Albert: Column 17 Line 7 – 11 & Figure 2 / Element 500: an host computer at a remote location via a wireless network relative to said smartcard reader).

However, Albert does not disclose expressly a smartcard reader for encrypting a data signal.

Baratelli teaches a smartcard reader for encrypting a data signal (Baratelli: Column 7 Line 35 – 44: WRU (Write / Read Unit) of a smart card transmits encrypted data signal using private / public key mechanisms).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Baratelli within the system of Albert because (a) Albert teaches reading the identifying data from a smart card as a financial transaction device for authentication purpose (Albert : Column 5 Line 25 – 35), and (b) Baratelli teaches an enhanced security mechanism of smart card system by first validating a biometric identity of an individual and subsequently encrypting the secure data with private / public keys for authentications (Baratelli : Column 1 Line 40 – 46 and Column 6 Line 46 – 55).

As per claim 2, Albert does not disclose expressly said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly.

Baratelli teaches said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly (Baratelli: Column 6 Line 31 – 38: fingerprint).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Baratelli within the system of Albert because (a) Albert teaches reading the identifying data from a smart card as a financial transaction device for authentication purpose (Albert : Column 5 Line 25 – 35), and (b) Baratelli teaches using a biometric identity of an individual to enhance the security check (Baratelli : Column 1 Line 40 – 46).

As per claim 17 and 30, Albert as modified teaches said smartcard contains biometric data and said smartcard reader comprises a biometric smartcard reader for obtaining biometric data directly (Baratelli: Column 6 Line 31 – 38: fingerprint).

As per claim 3, 18 and 31, Albert as modified teaches said biometric data comprises fingerprint data (Baratelli: Column 6 Line 31 – 38).

As per claim 4 and 19, Albert as modified teaches said biometric data is not transmitted to said remote location from said smartcard reader (Baratelli: Column 6 Line 46 – 56: only the signed challenge is used for remote authentication purpose after biometric data is locally validated).

As per claim 9, Albert does not disclose expressly encrypting communications between said smartcard and said smartcard reader.

Baratelli teaches encrypting communications between said smartcard and said smartcard reader (Baratelli: Column 6 Line 46 – 55 and Column 7 Line 35 – 44: the information between the smart card and WRU (Write / Read Unit) of a smart card is encrypted using private / public key mechanisms).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Baratelli within the system of Albert because (a) Albert teaches reading the identifying data from a smart card as a financial transaction device for authentication purpose (Albert : Column 5 Line 25 – 35), and (b) Baratelli teaches an enhanced security mechanism of smart card system by first validating a biometric identity of an individual and subsequently encrypting the secure data with security keys for authentications (Baratelli : Column 1 Line 40 – 46 and Column 6 Line 46 – 55).

As per claim 20, Albert as modified teaches providing access using said access mechanism if said translated signal is determined by said access controller to authorize access (Albert: Column 18 Line 62 – 67: the recovered digital data signal format is communicated with authorization processor to authorize access).

As per claim 21, Albert as modified teaches said access mechanism is able to provide access to at least one of a door, portal, computer, network, secure equipment and secure installation (Albert: Column 18 Line 62 – 67).

As per claim 22, Albert as modified teaches said access information comprises at least one of a person's name, a facility code, a company code, an access code, and an issue code (Albert: Column 5 Line 24 – 29).

As per claim 23, Albert as modified teaches said signal is encrypted using triple DES, Skipjack, or AES Rijndael encryption (Albert: Column 12 Line 40).

As per claim 24, Albert as modified teaches encrypting communications between said smartcard and said smartcard reader (Baratelli: Column 6 Line 46 – 55 and Column 7 Line 35 – 44: the information between the smart card and WRU (Write / Read Unit) of a smart card is encrypted using private / public key mechanisms).

As per claim 27, Albert as modified teaches said translated signal is in a controller-specified format (Albert: Column 18 Line 62 – 63 & Abstract Line 10 – 12: the host computer transform the format between the PSTN non-compatible format and PSTN compatible format (i.e. recovered digital data format) and thus the translated signal is the recovered digital data format, which is a PSTN compatible format used by authorization processor, i.e. access controller).

5. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Delp et al. (U.S. Patent 6,922,558).

As per claim 12, Albert does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers.

Delp teaches said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers (Delp: Column 18 Line 57 – 59: the maximum distance for 4000 feet = (0.3 m / ft.) x 4000 ft. = 1.2 km).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Delp within the system of Albert because (a) Albert teaches a network structure of a financial transaction authorization system that reads the identifying data from a local financial transaction device and validated remotely at the authorization processors (Albert : Column 5 Line 25 – 35 / Line 37 – 54 and Column 18 Line 65 – 67), and (b) Delp teaches providing various network infrastructures for a vender tracking system that can increase the total number of modules supported by the system and thus increase the coverage area including remote locations with cost reductions for installation and maintenance (Delp: Column 17 Line 21 – 25, Column 18 Line 62 – 67 and Abstract / Line 18 – 22).

6. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Bartholomew et al. (U.S. Patent 5,724,417).

As per claim 13, Albert does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 15 meters.

Bartholomew teaches said smartcard reader and said high security module are separated by a distance of up to 15 meters (Bartholomew : Column 4 Line 37 – 38 / Line 47 – 50: signal coverage over distances on the order of tens or hundreds of feet and thus includes 50 feet = (0.3 m / ft.) x 50 ft. = 15 meters).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bartholomew within the system of Albert because (a) Albert teaches a wireless network structure of a financial transaction authorization system that can remotely validate the identifying data read from a local financial transaction device, e.g. smart card, (Albert : Column 5 Line 25 – 35 / Line 37 – 54 and Column 18 Line 65 – 67), and (b) Bartholomew teaches providing a smart card wireless data communication capabilities with spanning moderate coverage distances (Bartholomew : Column 4 Line 37 – 50).

7. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Renner et al. (U.S. Patent 6,223,984).

As per claim 15, Albert does not teach said controller-specified format is Wiegand format, or clock and data.

Renner teaches said controller-specified format is Wiegand format, or clock and data (Renner: Column 4 Line 9 – 11 and Column 6 Line 11 – 15: Wiegand format)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Renner within the system of Albert because (a) Albert teaches reading the identifying data from a smart card as a financial transaction device for authentication purpose (Albert : Column 5 Line 25 – 35), and (b) Renner teaches an effective mechanism to resolve the format compatibility issues across different smart card holders without making major modifications to cash register or ATM (Renner : Column 2 Line 23 – 32 and Column 3 Line 49 – 53).

8. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Baratelli (U.S. Patent 6,325,285), and in view of Delp et al. (U.S. Patent 6,922,558).

As per claim 25, Albert as modified does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers.

Delp teaches said smartcard reader and said high security module are separated by a distance of up to 1.2 kilometers (Delp: Column 18 Line 57 – 59: the maximum distance for 4000 feet = (0.3 m / ft.) x 4000 ft. = 1.2 km).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Delp within the system of Albert as modified because (a) Albert teaches a network structure of a financial transaction authorization system that reads the identifying data from a local financial transaction device and validated remotely at the authorization processors (Albert : Column 5 Line 25 – 35 / Line 37 – 54 and Column 18 Line 65 – 67), and (b) Delp teaches providing various network infrastructures for a vender tracking system that can increase the total number of modules supported by the system and thus increase the coverage area including remote locations with cost reductions for installation and maintenance (Delp: Column 17

9. Claim 26 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Baratelli (U.S. Patent 6,325,285), and in view of Bartholomew et al. (U.S. Patent 5,724,417).

As per claim 26, Albert as modified does not disclose expressly said smartcard reader and said high security module are separated by a distance of up to 15 meters.

Bartholomew teaches said smartcard reader and said high security module are separated by a distance of up to 15 meters (Bartholomew : Column 4 Line 37 – 38 / Line 47 – 50: signal coverage over distances on the order of tens or hundreds of feet and thus includes 50 feet = (0.3 m / ft.) x 50 ft. = 15 meters).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bartholomew within the system of Albert as modified because (a) Albert teaches a wireless network structure of a financial transaction authorization system that can remotely validate the identifying data read from a local financial transaction device, e.g. smart card, (Albert : Column 5 Line 25 – 35 / Line 37 – 54 and Column 18 Line 65 – 67), and (b) Bartholomew teaches providing a smart card wireless data communication capabilities with spanning moderate coverage distances (Bartholomew : Column 4 Line 37 – 50).

10. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Albert et al. (U.S. Patent 5,991,410), in view of Baratelli (U.S. Patent 6,325,285), and in view of Renner et al. (U.S. Patent 6,223,984).

As per claim 28, Albert as modified does not teach said controller-specified format is Wiegand format, or clock and data.

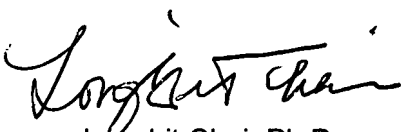
Renner teaches said controller-specified format is Wiegand format, or clock and data (Renner: Column 4 Line 9 – 11 and Column 6 Line 11 – 15: Wiegand format)

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Renner within the system of Albert as modified because (a) Albert teaches reading the identifying data from a smart card as a financial transaction device for authentication purpose (Albert : Column 5 Line 25 – 35), and (b) Renner teaches an effective mechanism to resolve the format compatibility issues across different smart card holders without making major modifications to cash register or ATM (Renner : Column 2 Line 23 – 32 and Column 3 Line 49 – 53).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Longbit Chai, Ph.D.
Patent Examiner
Art Unit 2131
7/2/2007